ABSTRACT

A method and apparatus for detecting viral code that uses calls to an operating system to damage computer systems, computers and/or computer files is provided. The apparatus comprises a CPU emulator, a memory manager component and a monitor component. An artificial memory region spanning one or more components of the operating system is created by the memory manager component. Execution of computer executable code in a subject file is emulated by the CPU emulator. An attempt by the emulated computer executable code to access the artificial memory region is detected by the monitor component. The apparatus optionally may comprise an auxiliary component and an analyzer component. The auxiliary component determines an operating system call that the emulated computer executable code attempted to access. The analyzer component monitors the operating system call to determine whether the computer executable code is viral.